



## Enhancement in Security Protocol of Spontaneous Wireless AD-hoc Network

**Kirti Dahiya\***

M.Tech, ECE Deptt., NCCE,  
Panipat, Haryana, India

**Jagtar Singh**

Senior Lecturer, ECE Deptt., NCCE,  
Panipat, Haryana, India

---

**Abstract**— *this paper presents an Enhanced secure protocol for spontaneous wireless ad hoc networks which uses a hybrid symmetric/ asymmetric scheme and the trust between users in order to exchange the initial data and to exchange the secret keys that will be used to encrypt the data. Trust is based on the first visual contact between users. Proposed protocol is secure autonomous protocol and is not based on any infrastructure and external support in order to develop it over the devices with limited resources. Network creation, communication and management are the functionalities of the proposed system. A mechanism has been presented to allow the nodes to check the authenticity of their IP addresses while not generating any duplicated IP addresses. This mechanism helps nodes to authenticate by using their IP addresses. The proposed protocol has the following features Distributed security mechanism, Lightweight, Malicious user revocation capability.*

**Keywords**— *Spontaneous Network, IDC, PDA, NS-2, PDR, MANET*

---

### I. INTRODUCTION

An wireless ad-hoc networks are decentralized in nature which makes them suitable for a variety of applications where central nodes can't relied on pre existing infrastructure and thus improve the scalability of networks compared to wireless managed networks, though theoretical and practical limits to the overall capacity of such networks have been identified. Thus minimal configuration and quick deployment makes ad hoc networks more suitable for emergency situations like natural disasters or military conflicts. The dynamic and adaptive routing protocols enable ad hoc networks to be formed quickly and spontaneously. Spontaneous ad hoc networks are those networks which use both hybrid symmetric and asymmetric scheme and also transfer data dynamically between different nodes of network

- Spontaneous ad hoc networks are formed by a set of mobile terminals which are placed in a close location and communicate with each other, share resources, services or computing time during a limited period of time and in a limited space, following human interaction pattern.
- People are attached to a group of people for a while, and then leave the network. Network management should be transparent to the user.
- A spontaneous network is a special case of ad hoc networks.
- They usually have little or no dependence on a centralized administration.

**Some of the advantages of spontaneous wireless ad-hoc network are as follow:**

#### **Lightweight Protocol**

As these networks are implemented in devices such as laptops, PDAs or mobile phones, with limited capacities thus they must use lightweight protocols and new methods to control, manage, and integrate them. The configuration services in spontaneous networks depend significantly on network size, the nature of the participating nodes and running applications. Spontaneous networks imitate human relations while having adaptability to new conditions and fault tolerance (the failure of a device or service should not damage the functionality). Methods based on imitating the behaviour of human relations facilitate secure integration of services in spontaneous networks. Furthermore, cooperation among the nodes and quality of service for all shared network services should be provided.

#### **Security Features**

Confidentiality, Node cooperation, anonymity and privacy.

#### **Constraints**

Energy constraints, node variability, error rate, and bandwidth limitations mandate the design and use of adaptive routing and security mechanisms, for any type of devices and scenarios. Dynamic networks with flexible memberships, group signatures, and distributed signatures are difficult to manage. To achieve a reliable communication and node authorization in mobile ad hoc networks, key exchange mechanisms for node authorization and user authentication are needed.

## Services

Group communication, collaboration in program delivery, security.

## II. LITERATURE REVIEW

Raquel Lacuesta, "A Spontaneous Ad Hoc Network to Share WWW Access" A secure spontaneous ad-hoc network is presented, which is based on direct peer-to-peer interaction, to grant a quick, easy, and secure access to the users to surf the Web. The literature shows the description of our proposal, the procedure of the nodes involved in the system, the security algorithms implemented, and the designed messages.

Ronald Watro, "TinyPK: Securing Sensor Networks with Public Key Technology" The design and implementation of public-key-(PK)-based protocols that allow authentication and key agreement between a sensor network and a third party as well as between two sensor networks. Our work is novel in that PK technology was commonly believed to be too inefficient for use on low-power devices. The TinyPK system demonstrates that a public-key based protocol is feasible for an extremely lightweight sensor network.

James Goodman, "An Energy-Efficient Reconfigurable Public-Key Cryptography Processor"

Given a specific domain of functionality such as public-key cryptography, it is possible to provide a limited degree of domain-specific re-configurability to provide flexibility while minimizing the overhead that is typically associated with reprogrammable logic. Domain specific integrated circuits (DSICs) utilize interconnect-centric architectures to exploit locality in order to minimize the interconnection overhead, which is the dominant source of energy consumption in generic reconfigurable logic.

Arvinderpal S. Wander, "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks"

In this literature, the energy cost of authentication and key exchange based on public-key cryptography on an 8-bit microcontroller platform has been quantified. A comparison of two public-key algorithms, RSA and Elliptic Curve Cryptography (ECC), has been presented and mutual authentication and key exchange between two untrusted parties are considered such as two nodes in a wireless sensor network.

Sencun Zhu, "LHAP: A Lightweight Network Access Control Protocol for Ad-Hoc Networks"

Most ad hoc networks do not implement any network access control, leaving these networks vulnerable to resource consumption attacks where a malicious node injects packets into the network with the goal of depleting the resources of the nodes relaying the packets. To thwart or prevent such attacks, it is necessary to employ authentication mechanisms to ensure that only authorized nodes can inject traffic into the network. A hop-by-hop authentication protocol called LHAP has been proposed for ad hoc networks.

## III. PROPOSED WORK

A simple security model for a sensor network employs a single secret key that is known by all nodes in the sensor network. There are many potential problems with this simple model and it clearly fails to scale to large systems. However, in a small local region of the sensor network, this simple model is likely to hold. The single shared secret key creates a communication crypto net: possession of the key authenticates the holder as part of the secure group. Traffic sent in the sensor network is encrypted and integrity protected using the common key. Since traffic is sometimes broadcast and sometimes routed hop-to-hop across the sensor network, the single encryption key provides very user friendly security architecture, albeit with the already mentioned limitations. This system uses the Centralized authority which affects the spontaneous nature of the network.

None of the existing systems propose a secure spontaneous network protocol based on user trust that provides node authenticity, integrity checking, and privacy and they require an initial configuration (i.e., network configuration) or external authorities (for example, central certification authorities). To solve the above issue, a novel protocol is proposed for the creation of spontaneous network and data distribution, sharing of resources, and services securely. Main objective of the spontaneous network creation is the integration of services and devices in the same environment, enabling the user to have instant service without any external infrastructure.

Proposed protocol is more secured and autonomous protocol which is not based on any infrastructure and external support in order to develop it over the devices with limited resources. Network creation, communication and management is the functionalities of the proposed system.

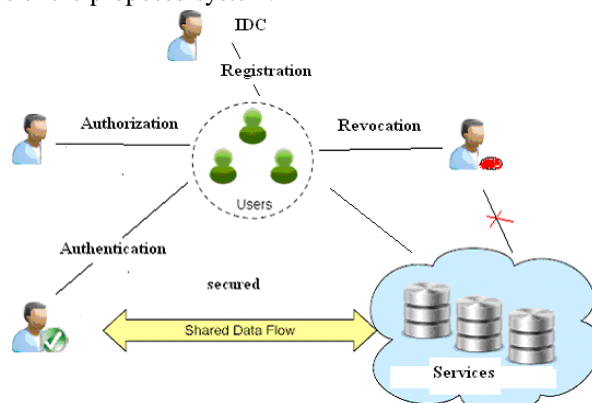


Fig 1: Secured Wireless Ad hoc Network

Initial data and key exchange is done based on trust between nodes. Data is exchanged securely by applying encryption over the data with key. Asymmetric cryptography, where each device has a public-private key pair for device identification and symmetric cryptography to exchange session keys between nodes. There are no anonymous users, because confidentiality and validity are based on user identification. Security is established based on the service required by the users, by building a trust network to obtain a distributed certification authority. A new user can be joined to the network only if he/she knows someone who belongs to the network. Certificate authority is distributed between the users who trust the new user. The network management is also distributed, which allows the network to have a distributed name service.

The proposed protocol has following features:

- Distributed security mechanism
- Lightweight
- Malicious user revocation capability

### **Malicious user revocation**

Each user in the network maintains the revocation list. Revocation list contains the identity of the attackers. If a user is identified as the attacker, he/she should be eliminated from the network. Particular user's unique identity is updated to the all the users existed in the network. All users in the network update their revocation list. When the attacker enters into the system for any service, revocation list is verified. If the user existed in the revocation list, that user will not get the service.

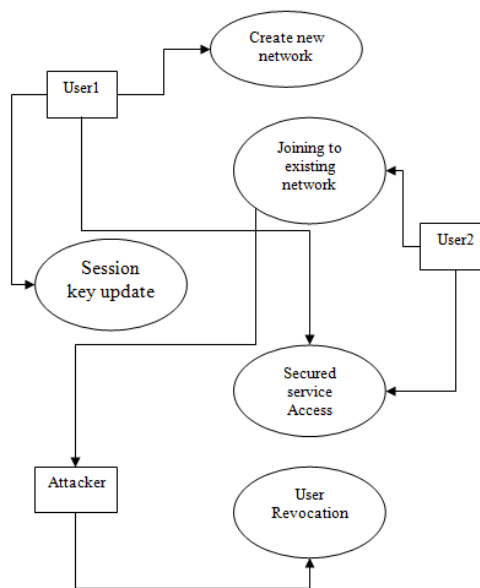


Fig 2: Flow chart of spontaneous secured network

Ad hoc network is basically infrastructure less in nature and it is vulnerable to attacks. In such a network it is necessary to create the security without autonomously and without the involvement of centralized architecture. To solve the above issue, a novel security protocol is proposed for the spontaneous network creation. Initial network creation is done based on trust. For each newly added user authorization is performed using certificate generation. Authentication is carried out using certificate verification mechanism. Session key is used by all the nodes in the network, for the secure communication. Symmetric key encryption is used for data encryption. Asymmetric cryptography is used for session key encryption and signature generation. Session key updating is carried out based on expiration time. To revoke the attacker from participating in the network, User revocation mechanism is contributed to the proposed security protocol. Hence security is enhanced with revocation capabilities.

**The presented work is divided in five stages:**

#### **1. Creating a new Network**

- 1a.Generation of IDC
- 1b.Generation of session key

#### **2. Joining to the existing network**

- 2a.Sharing IDC with signature using Cryptography algorithm
- 2b.Authorization: Certificate Generation to the new user

#### **3. Service Access**

- 3a.Authentication: Certificate Verification
- 3b.Secure session key sharing
- 3c.Secure Data Sharing

#### **4. Session Key Update**

#### **5. User Revocation**

#### IV. IMPLEMENTATION

NS-2 is a discrete event simulator which is written in C++, with an OTcl interpreter shell as the user interface that allows the input model files (Tcl scripts) to be executed. Most network elements in NS2 simulator are developed as classes, in object-oriented fashion. The simulator supports a class hierarchy in C++, and a very similar class hierarchy in OTcl. The root of this class hierarchy is the TclObject in.

The proposed algorithm is simulated in following steps

##### 1. Creating a new Network

- 1a. Generation of IDC
- 1b. Generation of session key

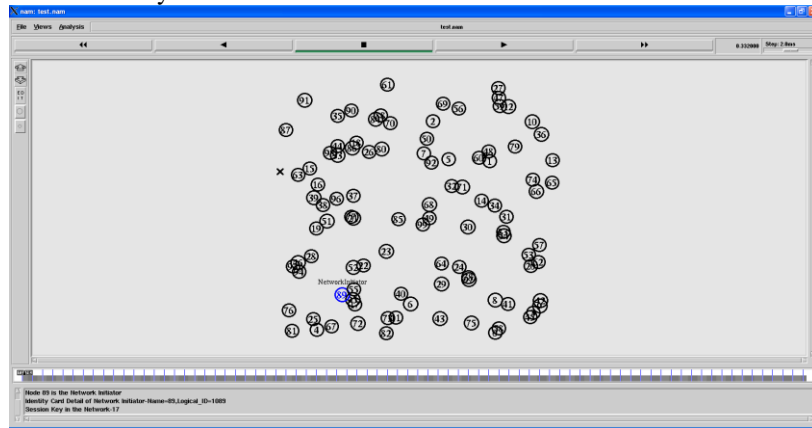


Fig 3: Generation of IDC and session key

Here figure 4.4 showing the data generation of IDC and session key over the network. The figure is showing that for creating a secured spontaneous network between the node pair of the network, node 89 acts as a network initiator, who will create a spontaneous network while session key is initiated by the node 17, which will be exchanged with new nodes after the authentication phase.

##### 2. Joining to the existing network

##### 2a. Sharing IDC with signature using Cryptography algorithm

Here figure 4 is showing that the requested IDC is shared with all the existing members of the network with signature by using cryptography algorithm. The above figure depicts that node 6 wants to joins the network therefore submit its IDC to network Initiator. Thereafter network member will encrypted the IDC and provide authentication and again network initiator will decrypts the member IDC for providing security in the network.

Network Member: 2

Name (6)=6

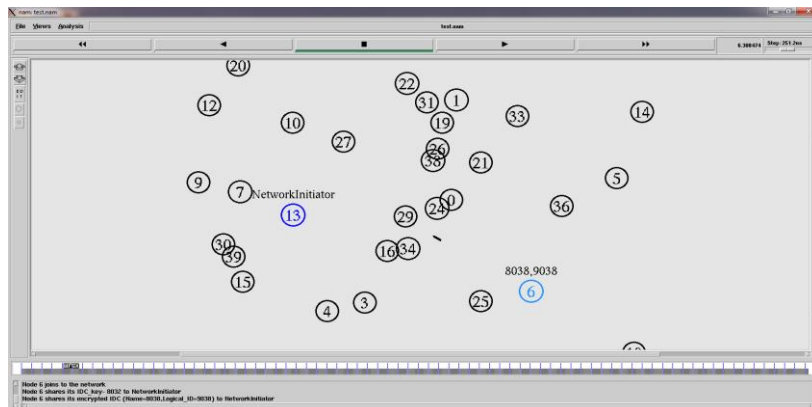


Fig 4: sharing of IDC using Cryptography algorithm

Logical\_ID (6)=1006

IDC key = 8032

Encrypted IDC:

Name=8038

Logical\_ID=9038

Network Initiator decrypts the member IDC

Decrypted IDC:

Name=6

Logical\_ID=1006

**2b. Authorization: Certificate Generation to the new user**

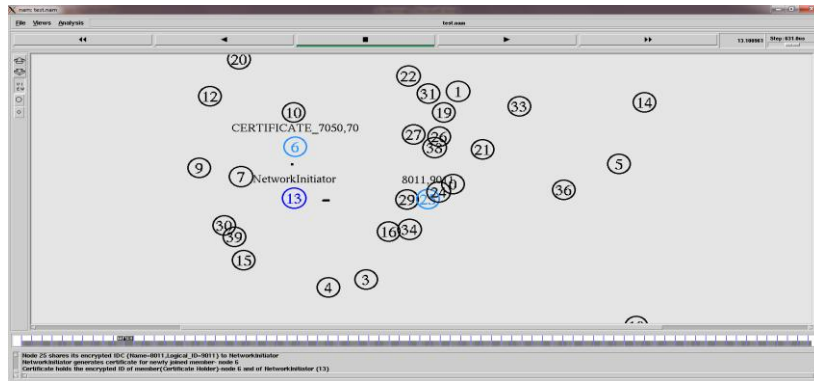


Fig 5: certification generation to the new user

Here figure 5 is showing that after verifying the network member, network Initiator decrypts the Encrypted IDC using the IDC key and when the decrypted IDC name is equal to the network member, network Initiator generates certificate for newly joined member. Thus certificate of validate IDC is issued by network initiator.

Certificate holds the encrypted ID of member (Certificate Holder) and of Network Initiator (Issuer).

Certificate of member: 6

Signing Key=7037

Issuer=7050

Holder=7043

**3. Service access**

**3a.Authentication: Certificate Verification.**

**3b.Secure session key sharing**

**3c.Secure Data Sharing**

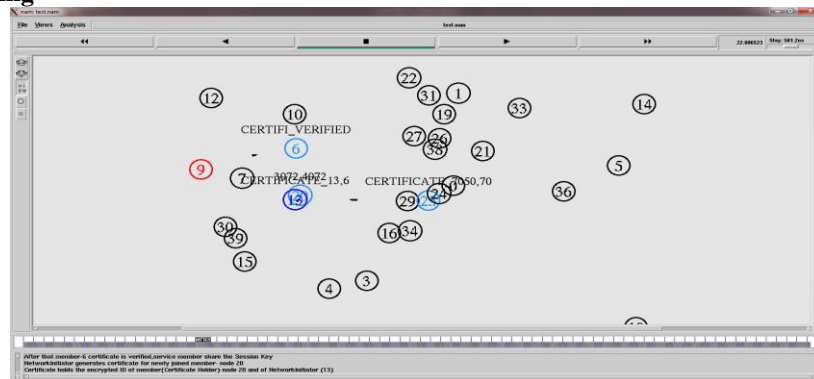


Fig 6: verification of issued certificate

Here figure 6 is showing that the Service providing user encrypts the data using the session key using symmetric encryption algorithm and sends it to Service requesting user. Service requesting user decrypts the data using session key. When network member node 6 (Requesting service member) gets the service from the any service member, first submitting the certificate to service member (node-25).

The service member (node-25) verifies the certificate of requesting service member 6.

If the verification of the Requesting member certificate is successful, it provided the service to its corresponding Requesting member node 6.

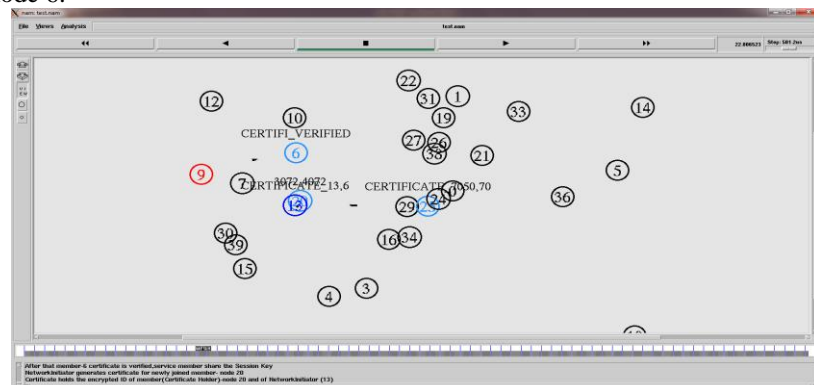


Fig 7 Verification of Certificate

Requesting\_Service\_Member:6  
 Service\_Member of node-6:25  
 Certificate\_Verification of member: 6  
 Decrypted\_Issuer=13  
 Decrypted\_Holder=6

Here figure 7 is showing that after verification of certificate, service is provided to the requested node. Here service member 25 is verified the certificate of request member (node 6), then it's provide the service to request member node 6. During the service (data) transmission, the data must encrypt and send to the corresponding request member (node 6). The data will be encrypted using the shared session key.

When the corresponding request member (node 6) received the encrypted data, it decrypts the data using the same session key.

Service\_Member\_25\_DATA

DATA:cefvfwqtpi

Encrypted Text:

dfgwgxrquj

Requesting\_Service\_Member\_6 (Access the data from node 25)

Decrypted Text:

cefvfwqtpi

## V. PERFORMANCE ANALYSIS

### Normalized routing overhead

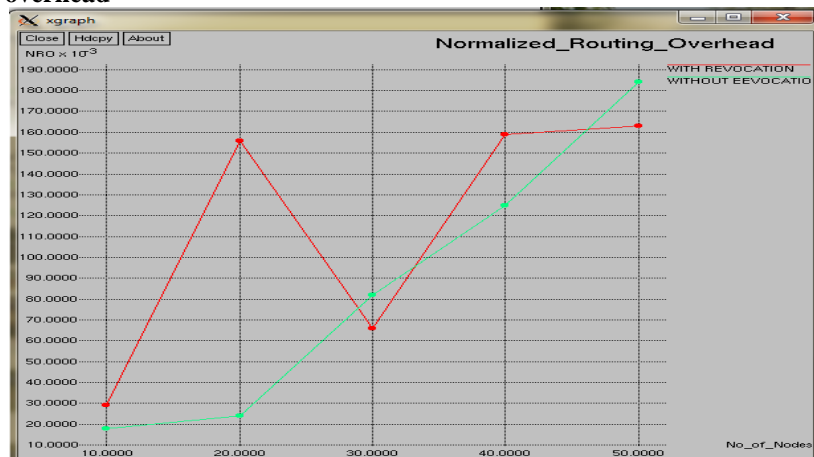


Fig 8: Normalized Routing Overhead Vs Number of Nodes

Here figure 8 is showing that Normalized routing Overhead with revocation is higher than that Normalized routing Overhead of without revocation. Because with revocation as the new user has to share control information for secure data services. Normalized routing overhead is more as compare to without revocation.

### Throughput

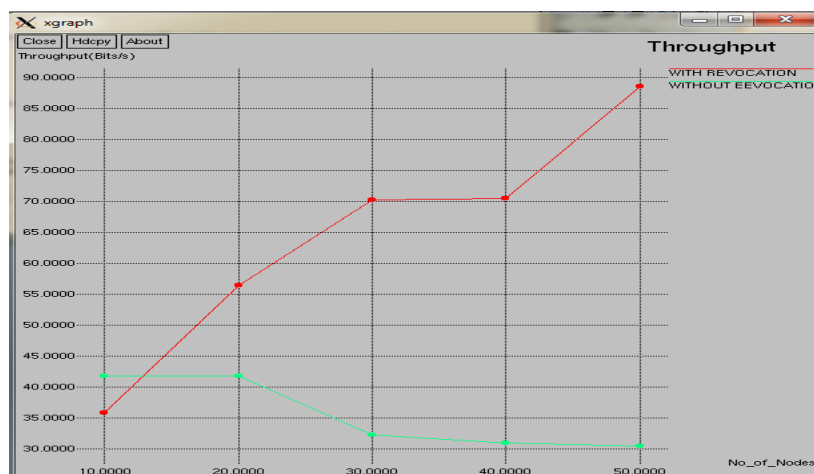


Fig 9: Throughput Vs Number of Nodes

Here figure 9 is showing that throughput of with revocation is higher than that of throughput of without revocation. In with revocation, when the attacker is detected, it eliminates the attacker in the network. Therefore attackers will not involve in the future.



### Packet Delivery Ratio

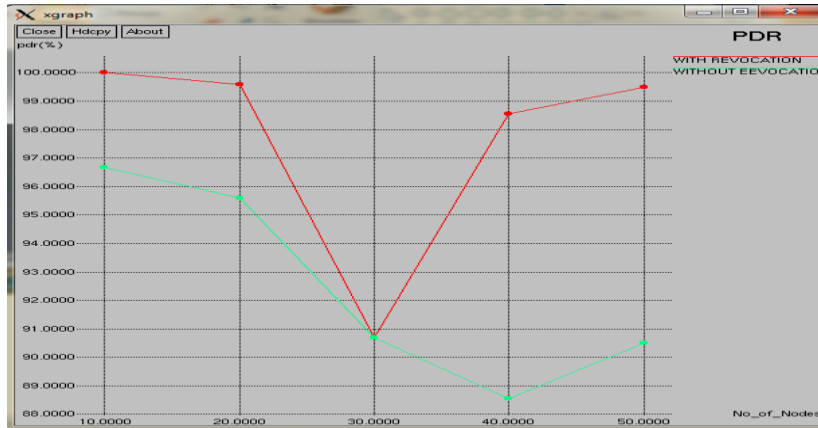


Fig 10: PDR Vs Number of Nodes

Here figure 10 is showing that Packet Delivery Ratio of with revocation is higher than that of Packet Delivery Ratio of without revocation. Because in without revocation list mechanism, the attacker is only detected, but it not eliminated from the network. Therefore a chance to this attacker affects the network. Thus if revocation list mechanism is used then attacker not only detected but is also removed from the network. Therefore Packet Delivery Ratio with revocation is better than without revocation.

### Average Delay



Fig 11: Average Delay Vs No. of Nodes

Here figure 11 shows that Average Delay of with revocation is lower than that of Average Delay of without revocation. Because in without revocation, the attacker is detected, but it not eliminated from the network. Therefore a chance to this attacker affects the network and causes a delay. Thus Average delay with revocation shows better result than without revocation.

## VI. CONCLUSION

In this paper, we show the design of an enhanced protocol that allows the creation and management of a spontaneous wireless ad hoc network. It is based on a social network imitating the behavior of human relationships. Thus, each user will work to maintain the network, improve the services offered, and provide information to other network users. We have enhanced the previous work by adding revocation method. We have also simulated the enhanced protocol of spontaneous network with revocation and without revocation and checked the performance of both with respect to packet delivery ratio, throughput, average delay, Normalized routing overhead and finds that with revocation method protocol performs better with respect to without revocation. A user without advanced technical knowledge can set up and participate in a spontaneous network. The security schemes included in the protocol allow secure communication between end users (bearing in mind the resource, processing, and energy limitations of ad hoc devices).

## REFERENCES

- [1] Raquel Lacuesta, Jaime Lloret, Senior Member, IEEE, A Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation IEEE transaction on parallel and distributed systems, vol. 24,no. 4,april 2013
- [2] R. Lacuesta, J. Lloret, M. Garcia, and L. Pen˜ alver, "A Spontaneous Ad-Hoc Network to Share WWW Access," EURASIP J. Wireless Comm. and Networking, vol. 2010, article 18, 2010.
- [3] V. Kumar and M.L. Das, "Securing Wireless Sensor Networks with Public Key Techniques," Ad Hoc and Sensor Wireless Networks, vol. 5, nos. 3/4, pp. 189-201, 2008.

- [4] J. Goodman and A. Chandrakasan, "An Energy Efficient Reconfigurable Public-Key Cryptography Processor Architecture," Proc. Int'l Workshop Cryptographic Hardware and Embedded Systems (CHES '00), pp. 175-190, 2000.
- [5] A. Wander, N. Gura, H. Eberle, V. Gupta, and S. Chang, "Energy Analysis for Public-Key Cryptography for Wireless Sensor Networks," Proc. IEEE Third Int'l Conf. Pervasive Computing and Comm. (PerCom '05), pp. 8-12, Mar. 2005.
- [6] V. Untz, M. Heusse, F. Rousseau, and A. Duda, "Lilith: an Interconnection Architecture Based on Label Switching for Spontaneous Edge Networks," Proc. First Ann. Int'l Conf. Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous '04), Aug. 2004.
- [7] S. Zhu, S. Xu, S. Setia, and S. Jajodia, "LHAP: A Lightweight Hopby- Hop Authentication Protocol For Ad-Hoc Networks," Ad Hoc Networks J., vol. 4, no. 5, pp. 567-585, Sept. 2006.
- [8] A. Noack and S. Spitz, "Dynamic Threshold Cryptosystem without Group Manager," Network Protocols and Algorithms, vol. 1, no. 1, Oct. 2009.
- [9] J. Yan, J. Ma, F. Li, and S.J. Moon, "Key Pre-distribution Scheme with Node Revocation for Wireless Sensor Networks," Ad Hoc and Sensor Wireless Networks, vol. 10, nos. 2/3, pp. 235-251, 2010.
- [10] M. Mukesh and K.R. Rishi, "Security Aspects in Mobile Ad Hoc Network (MANETs): Technical Review," Int'l J. Computer Applications, vol. 12, no. 2, pp. 37-43, Dec. 2010.
- [11] K. Sahadevaiah and P.V.G.D. Prasad Reddy, "Impact of Security Attacks on a New Security Protocol for Mobile Ad Hoc Networks," Network Protocols and Algorithms, vol 3, no. 4, pp. 122-140, 2011.
- [12] L. Herrero and R. Lacuesta, "A Security Architecture Proposal for Spontaneous Networks," Proc. Int'l Conf. Advances in the Internet Processing System and Interdisciplinary Research, Oct. 2003.
- [13] R. Lacuesta and L. Pen~ aver, "IP Addresses Configuration in Spontaneous Networks," Proc. Ninth WSEAS Int'l Conf. Computers (ICCOMP '05), July 2005.
- [14] R. Lacuesta and L. Pen~ alver, "Automatic Configuration of Ad-Hoc Networks: Establishing Unique IP Link-Local Addresses," Proc.Int'l Conf. Emerging Security Information, Systems and Technologies